

Exhibit 13

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

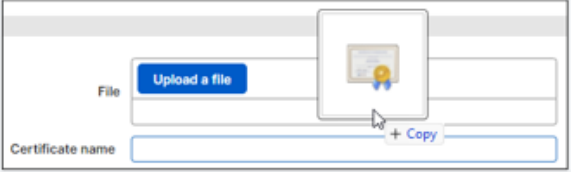
Exhibit 13 – U.S. Patent No. 9,294,470

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
<p>[1pre] A method of regulating population of a certificate store in a memory of a device, the method comprising:</p>	<p>Sophos Mobile is used to populate a certificate store in a memory of a device (e.g., a mobile device), e.g., for storing a certificate authority (CA) and certificates for use on mobile devices with Android Enterprise Work Profile.</p> <div data-bbox="699 488 1724 1138"> <p>Root certificate configuration (Android Enterprise work profile policy)</p> <p>Jul 4, 2023</p> <p>With the Root certificate configuration, you upload a root certificate to a policy. When you assign the policy to a device, the certificate gets installed in the Android work profile.</p> <p>You can upload X.509 certificate files in Privacy-Enhanced Mail (PEM) and Distinguished Encoding Rules (DER) encoding.</p> <p>Commonly used file extensions are:</p> <ul style="list-style-type: none"> • PEM encoding: .cer, .crt, .pem • DER encoding: .cer, .der <p>After you add a Root certificate configuration to a policy, you can use it in other configurations of the same policy, for example, as Extensible Authentication Protocol (EAP) server certificate in a Wi-Fi configuration.</p> </div> <p>https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/RootCert/index.html</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
	<p>Sophos Mobile is used to populate a certificate store in a memory of a device (e.g., a mobile device), e.g., for storing a certificate authority (CA) and certificates for use on mobile devices with Android Enterprise Work Profile.</p> <div data-bbox="808 414 1606 1117"> <p>Upload certificate</p> <p>For a general description of adding configurations to a policy, see Create policy.</p> <p>To upload a root certificate to a policy, do as follows:</p> <ol style="list-style-type: none"> 1. On the policy's Edit policy page, click Add configuration > Root certificate. 2. Click Upload a file. 3. Select a file containing a certificate in X.509 format and click Open. <p>Tip: Instead of using Upload a file, you can drag the certificate file from File Explorer and drop it anywhere in the File area.</p>  <ol style="list-style-type: none"> 4. After the file is uploaded, the Certificate name field shows the certificate issuer's Distinguished Name (DN) information. 5. Click Apply to save the configuration. 6. On the Edit policy page, click Save. <p>To upload more root certificates, add a Root certificate configuration for each certificate to the policy.</p> </div> <p>https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/RootCert/index.html</p>

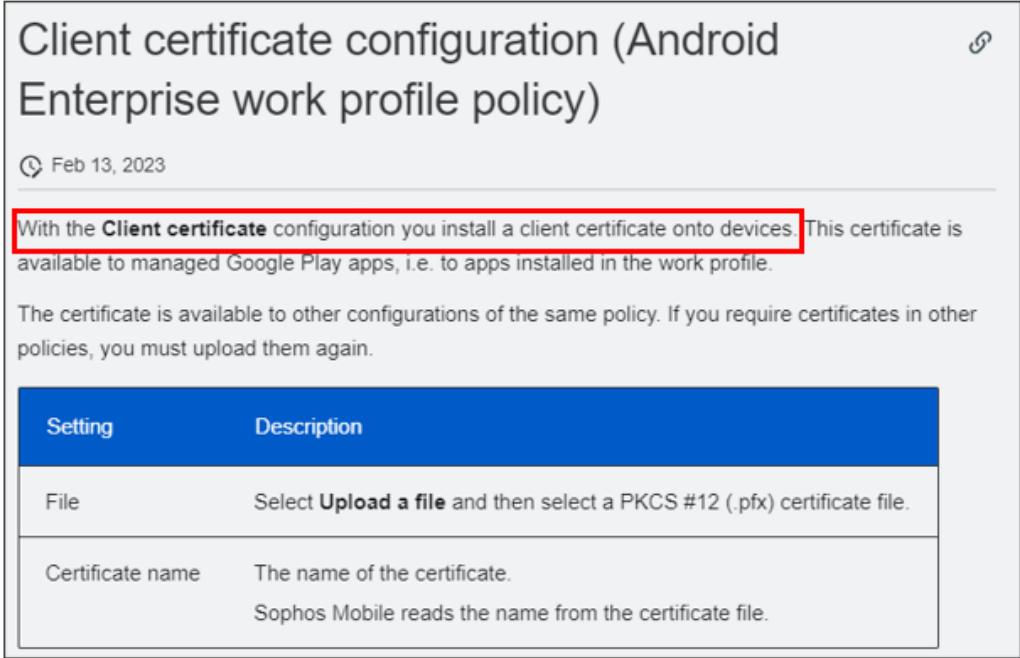
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
	<p>Sophos Mobile is used to populate a certificate store in a memory of a device (e.g., a mobile device), e.g., for storing a certificate authority (CA) and certificates for use on mobile devices with Android Enterprise Work Profile.</p> <div data-bbox="741 423 1659 1055"> <p><u>Use Sophos Mobile to install the root CA on mobile devices</u></p> <p>🕒 Apr 3, 2023</p> <p>You can add the Certificate Authority (CA) you configure for web or email protection to users' mobile devices remotely.</p> <p>This prevents untrusted certificate errors that occur when you apply a signing CA to SSL/TLS inspection and HTTPS decryption, and email TLS configurations.</p> <p>You can add the CA to users' endpoints remotely using Active Directory or a Mobile Device Management (MDM) solution.</p> <p>Apple recommends using an MDM solution or Apple Configurator to install the CA. If you do this, the CA is automatically trusted. If you use Apple Configurator, you must create a configuration profile on MacOS. You can then connect one or more iOS devices and install the CA on them.</p> <p>Using Sophos Mobile, our MDM solution, you can install certificates and CAs on groups of Android and iOS mobile devices. This example shows how to install the CA in iOS mobile devices enrolled with Sophos Mobile.</p> </div> <p>https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Certificates/HowToArticles/CertificatesInstallRootCAUsingSophosMobile/index.html</p>



Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification						
	<p data-bbox="619 321 1837 407">Sophos Mobile is used to populate a certificate store in a memory of a device (e.g., a mobile device), e.g., for storing a certificate authority (CA) and certificates for use on mobile devices with Android Enterprise Work Profile.</p> <div data-bbox="711 456 1724 1110">  <p>The screenshot shows the 'Client certificate configuration (Android Enterprise work profile policy)' page. It includes a date 'Feb 13, 2023' and a paragraph where 'Client certificate' is highlighted in a red box. Below this is a table with two rows: 'File' and 'Certificate name', each with a description. The table has a blue header with 'Setting' and 'Description'.</p> <table border="1"> <thead> <tr> <th>Setting</th><th>Description</th></tr> </thead> <tbody> <tr> <td>File</td><td>Select Upload a file and then select a PKCS #12 (.pfx) certificate file.</td></tr> <tr> <td>Certificate name</td><td>The name of the certificate. Sophos Mobile reads the name from the certificate file.</td></tr> </tbody> </table> </div> <p data-bbox="619 1133 1780 1157">https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/ClientCert/index.html</p>	Setting	Description	File	Select Upload a file and then select a PKCS #12 (.pfx) certificate file.	Certificate name	The name of the certificate. Sophos Mobile reads the name from the certificate file.
Setting	Description						
File	Select Upload a file and then select a PKCS #12 (.pfx) certificate file.						
Certificate name	The name of the certificate. Sophos Mobile reads the name from the certificate file.						

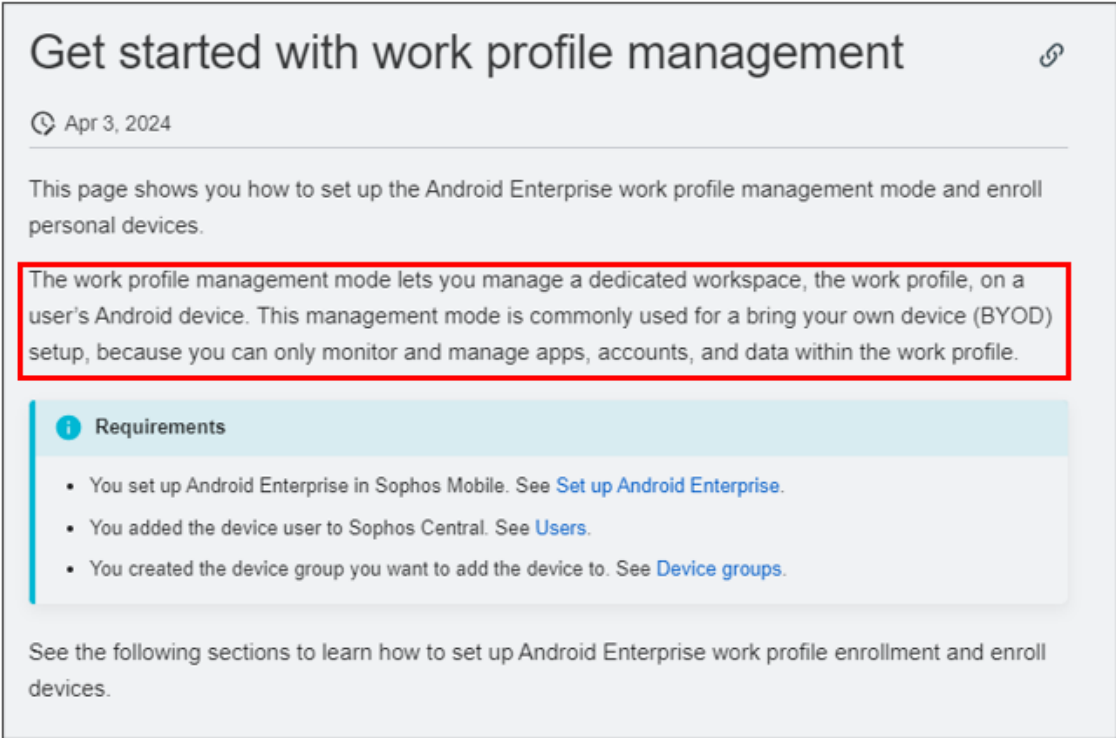
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
	<p data-bbox="615 318 1871 407">Sophos Mobile is used to populate a certificate store in a memory of a device (e.g., a mobile device), e.g., for storing a certificate authority (CA) and certificates for use on mobile devices with Android Enterprise Work Profile.</p> <div data-bbox="711 532 1736 875"><p data-bbox="726 553 1640 662">SCEP configuration (Android Enterprise work profile policy) </p><p data-bbox="726 691 877 716"> Feb 13, 2023</p><p data-bbox="726 756 1703 850">With the SCEP configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP). These certificates are available to apps that are installed in the work profile.</p></div> <p data-bbox="615 1151 1759 1175">https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/SCEP/index.html</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
	<p data-bbox="617 318 1877 378">Sophos Mobile is used with Android Enterprise Work Profile to manage a “work profile,” including regulating the certificate store of the work profile.</p> <div data-bbox="697 407 1806 1141">  <p data-bbox="722 435 1598 483">Get started with work profile management</p> <p data-bbox="722 516 867 540">Apr 3, 2024</p> <p data-bbox="722 581 1734 641">This page shows you how to set up the Android Enterprise work profile management mode and enroll personal devices.</p> <p data-bbox="722 670 1745 768" style="border: 2px solid red;">The work profile management mode lets you manage a dedicated workspace, the work profile, on a user's Android device. This management mode is commonly used for a bring your own device (BYOD) setup, because you can only monitor and manage apps, accounts, and data within the work profile.</p> <p data-bbox="751 816 921 841">Requirements</p> <ul data-bbox="760 878 1476 984" style="list-style-type: none"> • You set up Android Enterprise in Sophos Mobile. See Set up Android Enterprise. • You added the device user to Sophos Central. See Users. • You created the device group you want to add the device to. See Device groups. <p data-bbox="722 1044 1734 1104">See the following sections to learn how to set up Android Enterprise work profile enrollment and enroll devices.</p> </div> <p data-bbox="669 1154 1835 1175">https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/EnrollDevices/AndroidEnterprise/WorkProfileGetStarted/index.html</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification						
	<p>Sophos Mobile is used with Android Enterprise Work Profile to manage a “work profile,” including regulating the certificate store of the work profile. Sophos Mobile provides a setting to restrict or allow users to install or remove certificates in the work profile.</p> <div data-bbox="709 516 1743 901"><p>Security</p><table><tr><th>Setting</th><th>Description</th></tr><tr><td>Allow screen capture</td><td>Users can capture the screen content of apps installed in the work profile.</td></tr><tr><td>Allow user to configure credentials</td><td>Users can install or remove certificates in the work profile.</td></tr></table></div> <p>https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/Restrictions/index.html</p>	Setting	Description	Allow screen capture	Users can capture the screen content of apps installed in the work profile.	Allow user to configure credentials	Users can install or remove certificates in the work profile.
Setting	Description						
Allow screen capture	Users can capture the screen content of apps installed in the work profile.						
Allow user to configure credentials	Users can install or remove certificates in the work profile.						

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification														
	<p data-bbox="611 280 1871 342">Sophos Mobile is used with Android Enterprise Work Profile to manage a “work profile,” including regulating the certificate store of the work profile.</p> <div data-bbox="611 386 1864 1084"> <p data-bbox="621 402 974 440">Device management</p> <table data-bbox="621 459 1843 1068"> <thead> <tr> <th data-bbox="621 459 953 513">Feature</th><th data-bbox="953 459 1843 513">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="621 513 953 570">Configure Wi-Fi settings</td><td data-bbox="953 513 1843 570">Remotely deploy Wi-Fi login settings (SSID, password) to a device.</td></tr> <tr> <td data-bbox="621 570 953 662">Configure certificate-authenticated Wi-Fi</td><td data-bbox="953 570 1843 662">Remotely deploy Wi-Fi settings to a device that include identity, certificates for client authorization, and CA certificates.</td></tr> <tr> <td data-bbox="621 662 953 755">Restrict access to authorized accounts</td><td data-bbox="953 662 1843 755">Ensure that only authorized corporate accounts can interact with Work Profiles data by preventing users from adding or modifying accounts.</td></tr> <tr> <td data-bbox="621 755 953 847">Manage certificates</td><td data-bbox="953 755 1843 847">Deploy identity certificates and certificate authorities to a device to enable access to corporate resources.</td></tr> <tr> <td data-bbox="621 847 953 979">Manage advanced certificate details</td><td data-bbox="953 847 1843 979">Select certificates for specific work apps, remove CAs and identity certs from an active device, and <u>prevent users from modifying credentials in the managed keystore.</u></td></tr> <tr> <td data-bbox="621 979 953 1068">Enable Always On VPN</td><td data-bbox="953 979 1843 1068">Enable Always On VPN for specified apps in a Work Profile to ensure they always go through a configured VPN.</td></tr> </tbody> </table> </div> <p data-bbox="636 1101 1843 1125">https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features`</p>	Feature	Description	Configure Wi-Fi settings	Remotely deploy Wi-Fi login settings (SSID, password) to a device.	Configure certificate-authenticated Wi-Fi	Remotely deploy Wi-Fi settings to a device that include identity, certificates for client authorization, and CA certificates.	Restrict access to authorized accounts	Ensure that only authorized corporate accounts can interact with Work Profiles data by preventing users from adding or modifying accounts.	Manage certificates	Deploy identity certificates and certificate authorities to a device to enable access to corporate resources.	Manage advanced certificate details	Select certificates for specific work apps, remove CAs and identity certs from an active device, and <u>prevent users from modifying credentials in the managed keystore.</u>	Enable Always On VPN	Enable Always On VPN for specified apps in a Work Profile to ensure they always go through a configured VPN.
Feature	Description														
Configure Wi-Fi settings	Remotely deploy Wi-Fi login settings (SSID, password) to a device.														
Configure certificate-authenticated Wi-Fi	Remotely deploy Wi-Fi settings to a device that include identity, certificates for client authorization, and CA certificates.														
Restrict access to authorized accounts	Ensure that only authorized corporate accounts can interact with Work Profiles data by preventing users from adding or modifying accounts.														
Manage certificates	Deploy identity certificates and certificate authorities to a device to enable access to corporate resources.														
Manage advanced certificate details	Select certificates for specific work apps, remove CAs and identity certs from an active device, and <u>prevent users from modifying credentials in the managed keystore.</u>														
Enable Always On VPN	Enable Always On VPN for specified apps in a Work Profile to ensure they always go through a configured VPN.														

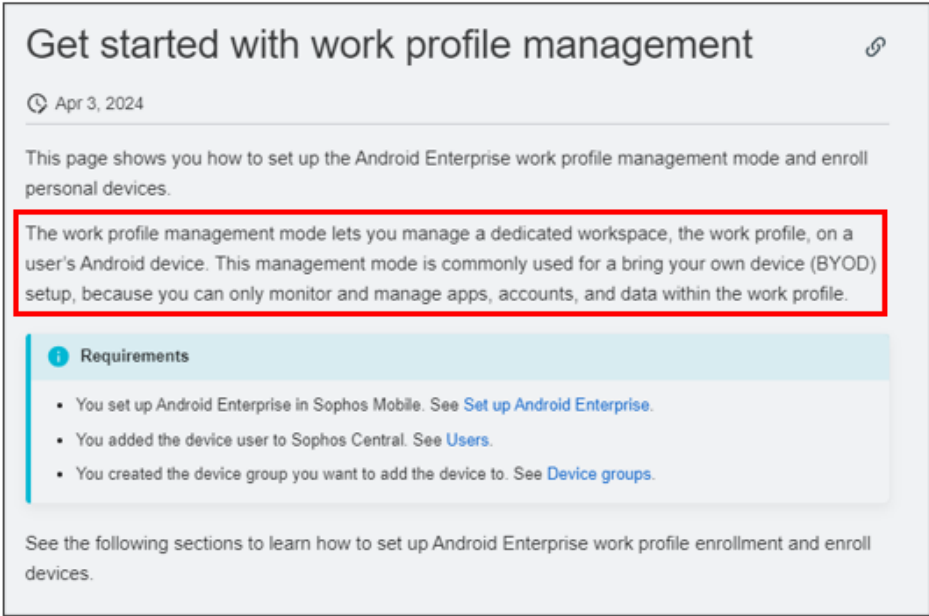
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification								
	<p>Sophos Mobile is used with Android Enterprise Work Profile to manage a “work profile,” including regulating the certificate store of the work profile.</p> <div><p>4.9. Advanced certificate management</p><table><tr><th>Android version</th><th>Work profile</th><th>Fully managed device</th><th>Dedicated device</th></tr><tr><td>7.0+</td><td>☆</td><td>☆</td><td>☆</td></tr></table><p>Allows IT admins to silently select the certificates that specific managed apps should use. This feature also grants IT admins the ability to remove CAs and identity certs from active devices, and prevent users from modifying credentials stored in the managed keystore.</p><p>4.9.1. For any app distributed to devices, IT admins can specify a certificate the app will be silently granted access during runtime. <i>(This subfeature is not currently supported)</i></p><ul style="list-style-type: none">• Certificate selection must be generic enough to allow a single configuration that applies to all users, each of which may have a user-specific identity certificate.<p>4.9.2. IT admins can silently remove certificates from the managed keystore.</p><p>4.9.3. IT admins can silently uninstall a CA certificate. <i>(This subfeature is not currently supported)</i></p><p><u>4.9.4. IT admins can prevent users from configuring credentials (go to <code>credentialsConfigDisabled</code>) in the managed keystore.</u></p><p>4.9.5. IT admins can pre-grant certificates for work apps using ChoosePrivateKeyRule.</p></div> <p>https://developers.google.com/android/work/requirements</p>	Android version	Work profile	Fully managed device	Dedicated device	7.0+	☆	☆	☆
Android version	Work profile	Fully managed device	Dedicated device						
7.0+	☆	☆	☆						

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
<p>[1a] determining that a device administration server is present;</p>	<p>Sophos Mobile is used to enroll a device in Android Enterprise Work Profile, whereby the device determines that a device administration server (e.g., a server hosting Sophos endpoint management software, such as Sophos Central) is present for managing the work profile.</p> <div data-bbox="787 451 1711 1063">  </div> <p>https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/EnrollDevices/AndroidEnterprise/WorkProfileGetStarted/index.html</p>

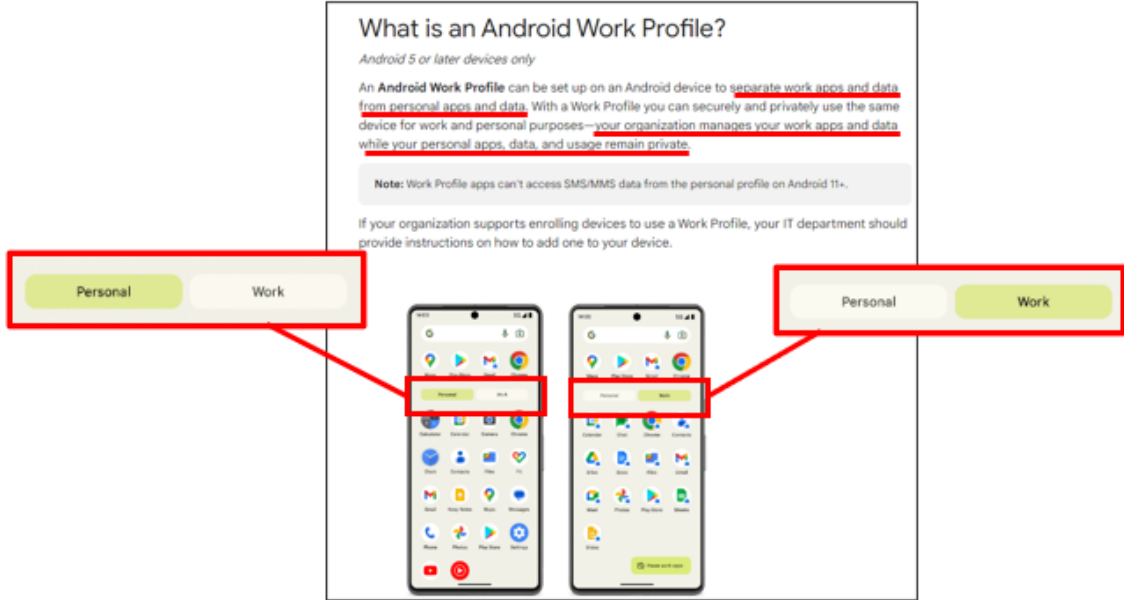
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
	<p data-bbox="615 282 1875 375">Sophos Mobile is used to enroll a device in Android Enterprise Work Profile, whereby the device determines that a device administration server (e.g., a server hosting Sophos endpoint management software, such as Sophos Central) is present for managing the work profile.</p> <div data-bbox="695 529 1791 967"><h3 data-bbox="737 558 1329 602">Work Profile and its features</h3><p data-bbox="737 626 1755 824"><u>A Work Profile is a self contained profile on an Android device for storing work apps and data. Work Profile allows separation of work apps and data, giving organizations full control of the data, apps, and security policies within a Work Profile. Simultaneously, users retain privacy over their personal apps, data, and usage.</u> On devices designated as company-owned during setup, organizations can enforce some policies that apply to a device's personal profile and overall device behavior.</p><p data-bbox="737 854 1745 946">Apps installed in the Work Profile are marked with the briefcase icon, so as to be easily distinguishable from personal apps. For more information on how to use a Work Profile device, see What is a Work Profile.</p></div> <p data-bbox="615 1078 1791 1138">https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
	<p data-bbox="617 282 1883 378">Sophos Mobile is used to enroll a device in Android Enterprise Work Profile, whereby the device determines that a device administration server (e.g., a server hosting Sophos endpoint management software, such as Sophos Central) is present for creating and managing the work profile.</p> <div data-bbox="659 492 1776 1089">  <p data-bbox="1014 505 1381 532">What is an Android Work Profile?</p> <p data-bbox="1014 542 1188 558"><i>Android 5 or later devices only</i></p> <p data-bbox="1014 570 1554 646">An Android Work Profile can be set up on an Android device to <u>separate work apps and data from personal apps and data</u>. With a Work Profile you can securely and privately use the same device for work and personal purposes—<u>your organization manages your work apps and data while your personal apps, data, and usage remain private</u>.</p> <p data-bbox="1031 667 1499 683">Note: Work Profile apps can't access SMS/MMS data from the personal profile on Android 11+.</p> <p data-bbox="1014 708 1560 743">If your organization supports enrolling devices to use a Work Profile, your IT department should provide instructions on how to add one to your device.</p> </div> <p data-bbox="932 1122 1575 1149">https://support.google.com/work/android/answer/6191949?hl=en</p>

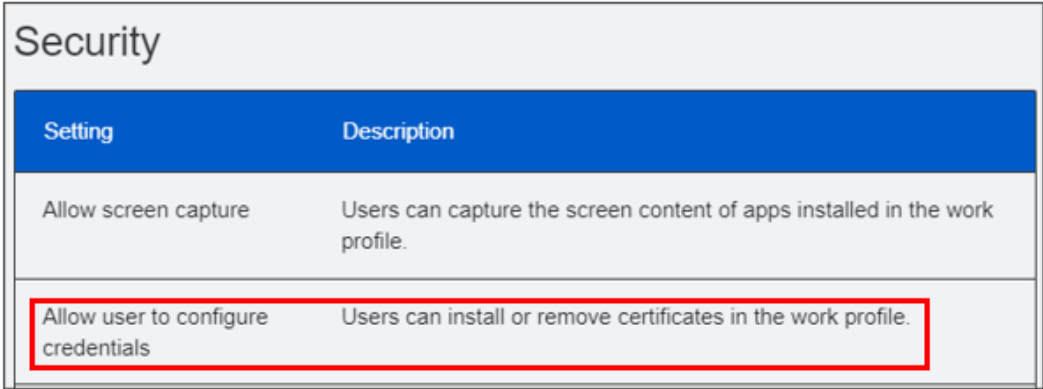
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
	<p data-bbox="611 289 1877 383">Sophos Mobile is used to enroll a device in Android Enterprise Work Profile, whereby the device determines that a device administration server (e.g., a server hosting Sophos endpoint management software, such as Sophos Central) is present for creating and managing the work profile.</p> <div data-bbox="795 448 1688 1065" style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"> <p data-bbox="835 461 1486 488">What policies can my organization manage on my device?</p> <p data-bbox="835 505 1638 646">When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile.</p> <p data-bbox="835 667 1591 719">If your device is personally-owned, your organization can carry out some or all of the following actions:</p> <ul data-bbox="835 740 1644 1065" style="list-style-type: none"> • <u>Remotely create, access, and delete data in your work profile</u> • Enforce minimum passcode requirements on your work profile and device • Change the password to your managed account (the account associated with your work profile) • Suspend access to your work profile • <u>Restrict what can be shared across your work and personal profiles</u> • <u>Block screen captures in your work profile</u> • <u>Manage access to your organization's corporate mail server and internal data</u> • <u>Remotely install (and uninstall) apps and certificates in your work profile</u> • <u>Manage permissions and other settings for apps in your work profile</u> </div> <p data-bbox="655 1130 1833 1157">https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification						
	<p data-bbox="617 282 1892 378">Sophos Mobile is used with Android Enterprise Work Profile to control whether users are able to modify credentials, including adding or deleting certificates for the work profile, whereby the device determines that an information technology policy for such control is enabled.</p> <div data-bbox="709 511 1745 898">  <table border="1"> <thead> <tr> <th>Setting</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Allow screen capture</td><td>Users can capture the screen content of apps installed in the work profile.</td></tr> <tr> <td>Allow user to configure credentials</td><td>Users can install or remove certificates in the work profile.</td></tr> </tbody> </table> </div> <p data-bbox="617 1122 1850 1149">https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/Restrictions/index.html</p>	Setting	Description	Allow screen capture	Users can capture the screen content of apps installed in the work profile.	Allow user to configure credentials	Users can install or remove certificates in the work profile.
Setting	Description						
Allow screen capture	Users can capture the screen content of apps installed in the work profile.						
Allow user to configure credentials	Users can install or remove certificates in the work profile.						

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification														
[1b] determining that an information technology policy is enabled; and	<p data-bbox="604 277 1885 375">Sophos Mobile is used with Android Enterprise Work Profile to control whether users <u>are able to modify credentials, including adding or deleting certificates for the work profile</u>, whereby the device determines that an information technology policy for such control is enabled.</p> <div data-bbox="615 391 1875 1089"> <h3 data-bbox="615 399 978 440">Device management</h3> <table border="1" data-bbox="615 459 1854 1081"> <thead> <tr> <th data-bbox="615 459 951 513">Feature</th><th data-bbox="951 459 1854 513">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="615 513 951 570">Configure Wi-Fi settings</td><td data-bbox="951 513 1854 570">Remotely deploy Wi-Fi login settings (SSID, password) to a device.</td></tr> <tr> <td data-bbox="615 570 951 659">Configure certificate-authenticated Wi-Fi</td><td data-bbox="951 570 1854 659">Remotely deploy Wi-Fi settings to a device that include identity, certificates for client authorization, and CA certificates.</td></tr> <tr> <td data-bbox="615 659 951 756">Restrict access to authorized accounts</td><td data-bbox="951 659 1854 756">Ensure that only authorized corporate accounts can interact with Work Profiles data by preventing users from adding or modifying accounts.</td></tr> <tr> <td data-bbox="615 756 951 846">Manage certificates</td><td data-bbox="951 756 1854 846">Deploy identity certificates and certificate authorities to a device to enable access to corporate resources.</td></tr> <tr> <td data-bbox="615 846 951 984">Manage advanced certificate details</td><td data-bbox="951 846 1854 984">Select certificates for specific work apps, remove CAs and identity certs from an active device, and <u>prevent users from modifying credentials in the managed keystore.</u></td></tr> <tr> <td data-bbox="615 984 951 1081">Enable Always On VPN</td><td data-bbox="951 984 1854 1081">Enable Always On VPN for specified apps in a Work Profile to ensure they always go through a configured VPN.</td></tr> </tbody> </table> </div> <p data-bbox="625 1114 1854 1138">https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>	Feature	Description	Configure Wi-Fi settings	Remotely deploy Wi-Fi login settings (SSID, password) to a device.	Configure certificate-authenticated Wi-Fi	Remotely deploy Wi-Fi settings to a device that include identity, certificates for client authorization, and CA certificates.	Restrict access to authorized accounts	Ensure that only authorized corporate accounts can interact with Work Profiles data by preventing users from adding or modifying accounts.	Manage certificates	Deploy identity certificates and certificate authorities to a device to enable access to corporate resources.	Manage advanced certificate details	Select certificates for specific work apps, remove CAs and identity certs from an active device, and <u>prevent users from modifying credentials in the managed keystore.</u>	Enable Always On VPN	Enable Always On VPN for specified apps in a Work Profile to ensure they always go through a configured VPN.
Feature	Description														
Configure Wi-Fi settings	Remotely deploy Wi-Fi login settings (SSID, password) to a device.														
Configure certificate-authenticated Wi-Fi	Remotely deploy Wi-Fi settings to a device that include identity, certificates for client authorization, and CA certificates.														
Restrict access to authorized accounts	Ensure that only authorized corporate accounts can interact with Work Profiles data by preventing users from adding or modifying accounts.														
Manage certificates	Deploy identity certificates and certificate authorities to a device to enable access to corporate resources.														
Manage advanced certificate details	Select certificates for specific work apps, remove CAs and identity certs from an active device, and <u>prevent users from modifying credentials in the managed keystore.</u>														
Enable Always On VPN	Enable Always On VPN for specified apps in a Work Profile to ensure they always go through a configured VPN.														

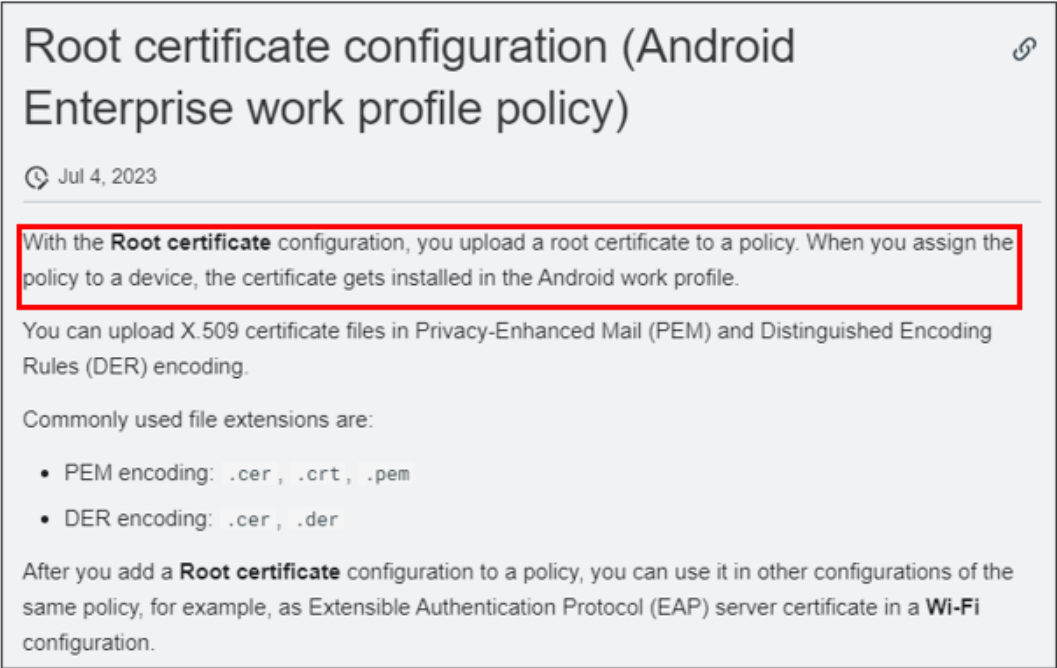
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification								
	<p>Sophos Mobile is used with Android Enterprise Work Profile to control whether users <u>are able to modify credentials</u>, including adding or deleting certificates for the work profile, whereby the device determines that an information technology policy for such control is enabled.</p> <div><p>4.9. Advanced certificate management</p><table><tr><th>Android version</th><th>Work profile</th><th>Fully managed device</th><th>Dedicated device</th></tr><tr><td>7.0+</td><td>☆</td><td>☆</td><td>☆</td></tr></table><p>Allows IT admins to silently select the certificates that specific managed apps should use. This feature also grants IT admins the ability to remove CAs and identity certs from active devices, and prevent users from modifying credentials stored in the managed keystore.</p><p>4.9.1. For any app distributed to devices, IT admins can specify a certificate the app will be silently granted access during runtime. <i>(This subfeature is not currently supported)</i></p><ul style="list-style-type: none">• Certificate selection must be generic enough to allow a single configuration that applies to all users, each of which may have a user-specific identity certificate.<p>4.9.2. IT admins can silently <u>remove certificates</u> from the managed keystore.</p><p>4.9.3. IT admins can silently uninstall a CA certificate. <i>(This subfeature is not currently supported)</i></p><p><u>4.9.4. IT admins can prevent users from <u>configuring credentials</u> (go to <code>credentialsConfigDisabled</code>) in the managed keystore.</u></p><p>4.9.5. IT admins can pre-grant certificates for work apps using <code>ChoosePrivateKeyRule</code>.</p></div> <p>https://developers.google.com/android/work/requirements</p>	Android version	Work profile	Fully managed device	Dedicated device	7.0+	☆	☆	☆
Android version	Work profile	Fully managed device	Dedicated device						
7.0+	☆	☆	☆						



Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
<p>[1c] responsive to the determining that the device administration server is present and that an information technology policy is enabled, disabling user interface interaction, on the device, for importing certificates into a certificate store associated with a portion of memory of the device.</p>	<p>For example, when Sophos Mobile is used to enroll devices in Android Enterprise Work Profile, a certificate store associated with a portion of memory for storing certificates for the work profile is initialized.</p> <div data-bbox="695 415 1745 1079">  <p>Root certificate configuration (Android Enterprise work profile policy)</p> <p>Jul 4, 2023</p> <p>With the Root certificate configuration, you upload a root certificate to a policy. When you assign the policy to a device, the certificate gets installed in the Android work profile.</p> <p>You can upload X.509 certificate files in Privacy-Enhanced Mail (PEM) and Distinguished Encoding Rules (DER) encoding.</p> <p>Commonly used file extensions are:</p> <ul style="list-style-type: none"> • PEM encoding: .cer , .crt , .pem • DER encoding: .cer , .der <p>After you add a Root certificate configuration to a policy, you can use it in other configurations of the same policy, for example, as Extensible Authentication Protocol (EAP) server certificate in a Wi-Fi configuration.</p> </div> <p>https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/RootCert/index.html</p>

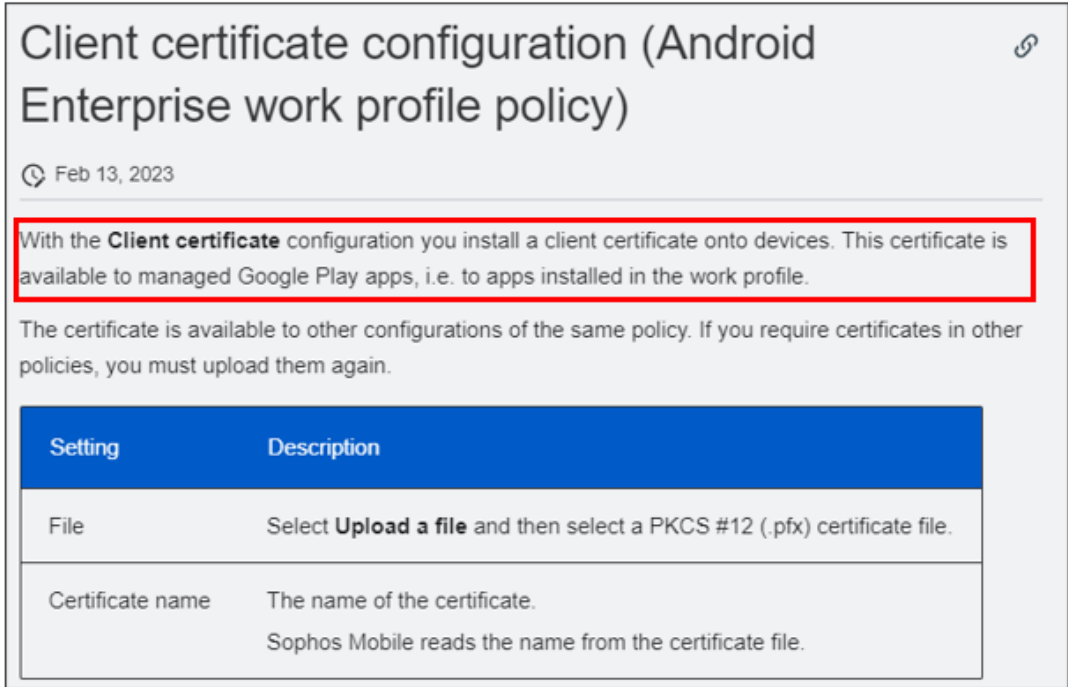
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
	<p data-bbox="615 321 1875 378">For example, when Sophos Mobile is used to enroll devices in Android Enterprise Work Profile, a certificate store associated with a portion of memory for storing certificates for the work profile is initialized.</p> <div data-bbox="709 410 1738 1117"> <p data-bbox="720 427 1606 532"><u>Use Sophos Mobile to install the root CA on mobile devices</u> </p> <p data-bbox="720 565 863 589"> Apr 3, 2023</p> <p data-bbox="720 630 1692 686">You can add the Certificate Authority (CA) you configure for web or email protection to users' mobile devices remotely.</p> <p data-bbox="720 719 1728 776">This prevents untrusted certificate errors that occur when you apply a signing CA to SSL/TLS inspection and HTTPS decryption, and email TLS configurations.</p> <p data-bbox="720 808 1602 865">You can add the CA to users' endpoints remotely using Active Directory or a Mobile Device Management (MDM) solution.</p> <p data-bbox="720 898 1728 987">Apple recommends using an MDM solution or Apple Configurator to install the CA. If you do this, the CA is automatically trusted. If you use Apple Configurator, you must create a configuration profile on MacOS. You can then connect one or more iOS devices and install the CA on them.</p> <p data-bbox="720 1019 1717 1109">Using Sophos Mobile, our MDM solution, you can install certificates and CAs on groups of Android and iOS mobile devices. This example shows how to install the CA in iOS mobile devices enrolled with Sophos Mobile.</p> </div> <p data-bbox="636 1125 1854 1182">https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Certificates/HowToArticles/CertificatesInstallRootCAUsingSophosMobile/index.html</p>



Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification						
	<p data-bbox="617 285 1881 345">For example, when Sophos Mobile is used to enroll devices in Android Enterprise Work Profile, a certificate store associated with a portion of memory for storing certificates for the work profile is initialized.</p> <div data-bbox="711 383 1772 1066">  <p data-bbox="726 402 1520 513">Client certificate configuration (Android Enterprise work profile policy)</p> <p data-bbox="726 542 884 570">Feb 13, 2023</p> <p data-bbox="726 607 1713 667">With the Client certificate configuration you install a client certificate onto devices. This certificate is available to managed Google Play apps, i.e. to apps installed in the work profile.</p> <p data-bbox="726 698 1724 758">The certificate is available to other configurations of the same policy. If you require certificates in other policies, you must upload them again.</p> <table border="1" data-bbox="726 786 1686 1053"> <thead> <tr> <th>Setting</th><th>Description</th></tr> </thead> <tbody> <tr> <td>File</td><td>Select Upload a file and then select a PKCS #12 (.pfx) certificate file.</td></tr> <tr> <td>Certificate name</td><td>The name of the certificate. Sophos Mobile reads the name from the certificate file.</td></tr> </tbody> </table> </div> <p data-bbox="617 1133 1829 1161">https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/ClientCert/index.html</p>	Setting	Description	File	Select Upload a file and then select a PKCS #12 (.pfx) certificate file.	Certificate name	The name of the certificate. Sophos Mobile reads the name from the certificate file.
Setting	Description						
File	Select Upload a file and then select a PKCS #12 (.pfx) certificate file.						
Certificate name	The name of the certificate. Sophos Mobile reads the name from the certificate file.						


Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
	<p data-bbox="615 321 1877 380">For example, when Sophos Mobile is used to enroll devices in Android Enterprise Work Profile, a certificate store associated with a portion of memory for storing certificates for the work profile is initialized.</p> <div data-bbox="699 540 1730 886"><p data-bbox="709 561 1633 672">SCEP configuration (Android Enterprise work profile policy) </p><p data-bbox="709 704 865 727"> Feb 13, 2023</p><p data-bbox="709 768 1703 865">With the SCEP configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP). These certificates are available to apps that are installed in the work profile.</p></div> <p data-bbox="615 1162 1772 1185">https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/SCEP/index.html</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
	<p data-bbox="617 280 1881 342">For example, when Sophos Mobile is used to enroll devices in Android Enterprise Work Profile, a certificate store associated with a portion of memory for storing certificates for the work profile is initialized.</p> <div data-bbox="766 370 1682 737" style="border: 2px solid red; padding: 10px;"> <p data-bbox="804 394 1297 435">Work Profile and its features</p> <p data-bbox="804 451 1654 618">A Work Profile is a self contained profile on an Android device for storing work apps and data. Work Profile allows separation of work apps and data, giving organizations full control of the data, apps, and security policies within a Work Profile. Simultaneously, users retain privacy over their personal apps, data, and usage. On devices designated as company-owned during setup, organizations can enforce some policies that apply to a device's personal profile and overall device behavior.</p> <p data-bbox="804 643 1640 721">Apps installed in the Work Profile are marked with the briefcase icon, so as to be easily distinguishable from personal apps. For more information on how to use a Work Profile device, see What is a Work Profile.</p> </div> <p data-bbox="646 745 1803 769">https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p> <div data-bbox="621 859 1875 1057" style="border: 1px solid black; padding: 10px;"> <p data-bbox="648 876 865 917">Work profile </p> <p data-bbox="1707 889 1829 906">Send feedback</p> <p data-bbox="648 963 1829 1040">The work profile solution set is intended for employee-owned devices and company-owned devices for work and personal use. Corporate apps, data, and management policies are restricted to the work profile. With a work profile, the same device can be used securely and privately for work and personal purposes.</p> </div> <p data-bbox="900 1060 1598 1084">https://developers.google.com/android/work/requirements/work-profile</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification
	<p data-bbox="617 282 1875 342">For example, when Sophos Mobile is used to enroll devices in Android Enterprise Work Profile, a certificate store associated with a portion of memory for storing certificates for the work profile is initialized.</p> <div data-bbox="617 565 772 587"> <p>Data segregation</p> </div> <p data-bbox="617 602 911 618">Work profiles use the following data segregation rules.</p> <p data-bbox="617 646 682 662">Apps ∞</p> <p data-bbox="617 678 1266 730">When the same app exists in the primary user and work profile, <u>apps are scoped with their own segregated data</u>. Generally, apps act independently and can't communicate directly with instances across the profile-user boundary unless they hold <code>INTERACT_ACROSS_PROFILES</code> permission or App-ops.</p> <p data-bbox="617 758 686 774">Accounts</p> <p data-bbox="617 790 1255 823">Accounts in the work profile are unique from the primary user and credentials can't be accessed across the profile-user boundary. Only apps in their respective context are able to access their respective accounts.</p> <p data-bbox="617 850 669 867">Intents</p> <p data-bbox="617 883 1232 915">The administrator controls whether intents are resolved in or out of the work profile. <u>By default, apps from the work profile are scoped to stay within the work profile exception of the Device Policy API.</u></p> <p data-bbox="642 937 1207 987">https://source.android.com/docs/devices/admin/managed-profiles</p> <div data-bbox="1297 548 1747 571"> <p>What policies can my organization manage on my device?</p> </div> <p data-bbox="1297 578 1848 672">When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile.</p> <p data-bbox="1297 688 1818 721">If your device is personally-owned, your organization can carry out some or all of the following actions:</p> <ul data-bbox="1297 737 1852 958" style="list-style-type: none"> • Remotely create, access, and delete data in your work profile • Enforce minimum passcode requirements on your work profile and device • Change the password to your managed account (the account associated with your work profile) • Suspend access to your work profile • Restrict what can be shared across your work and personal profiles • Block screen captures in your work profile • Manage access to your organization's corporate mail server and internal data • <u>Remotely install (and uninstall) apps and certificates in your work profile</u> • <u>Manage permissions and other settings for apps in your work profile</u> <p data-bbox="1297 976 1852 1055">https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification						
	<p data-bbox="611 285 1839 375">Responsive to a device being enrolled in Android Enterprise Work Profile and a policy to prevent modification of work profile certificates being enabled, user interface interaction on the device is disabled for importing certificates into the work profile certificate store.</p> <div data-bbox="701 505 1698 878"> <p data-bbox="709 524 856 565">Security</p> <table data-bbox="714 591 1694 872"> <thead> <tr data-bbox="714 591 1694 670"> <th data-bbox="714 591 1024 670">Setting</th><th data-bbox="1024 591 1694 670">Description</th></tr> </thead> <tbody> <tr data-bbox="714 670 1694 773"> <td data-bbox="714 670 1024 773">Allow screen capture</td><td data-bbox="1024 670 1694 773">Users can capture the screen content of apps installed in the work profile.</td></tr> <tr data-bbox="714 773 1694 872"> <td data-bbox="714 773 1024 872">Allow user to configure credentials</td><td data-bbox="1024 773 1694 872">Users can install or remove certificates in the work profile.</td></tr> </tbody> </table> </div> <p data-bbox="611 1094 1801 1118">https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/Policies/AndroidEnterpriseWorkProfile/Restrictions/index.html</p>	Setting	Description	Allow screen capture	Users can capture the screen content of apps installed in the work profile.	Allow user to configure credentials	Users can install or remove certificates in the work profile.
Setting	Description						
Allow screen capture	Users can capture the screen content of apps installed in the work profile.						
Allow user to configure credentials	Users can install or remove certificates in the work profile.						

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification														
	<p data-bbox="615 285 1829 375">Responsive to a device being enrolled in Android Enterprise Work Profile and a policy to prevent modification of work profile certificates being enabled, user interface interaction on the device is disabled for importing certificates into the work profile certificate store.</p> <div data-bbox="615 386 1829 1060"> <p data-bbox="625 402 968 440">Device management</p> <table border="1"> <thead> <tr> <th data-bbox="632 459 947 505">Feature</th><th data-bbox="947 459 1808 505">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="632 505 947 558">Configure Wi-Fi settings</td><td data-bbox="947 505 1808 558">Remotely deploy Wi-Fi login settings (SSID, password) to a device.</td></tr> <tr> <td data-bbox="632 558 947 651">Configure certificate-authenticated Wi-Fi</td><td data-bbox="947 558 1808 651">Remotely deploy Wi-Fi settings to a device that include identity, certificates for client authorization, and CA certificates.</td></tr> <tr> <td data-bbox="632 651 947 743">Restrict access to authorized accounts</td><td data-bbox="947 651 1808 743">Ensure that only authorized corporate accounts can interact with Work Profiles data by preventing users from adding or modifying accounts.</td></tr> <tr> <td data-bbox="632 743 947 836">Manage certificates</td><td data-bbox="947 743 1808 836">Deploy identity certificates and certificate authorities to a device to enable access to corporate resources.</td></tr> <tr> <td data-bbox="632 836 947 959">Manage advanced certificate details</td><td data-bbox="947 836 1808 959">Select certificates for specific work apps, remove CAs and identity certs from an active device, and <u>prevent users from modifying credentials in the managed keystore.</u></td></tr> <tr> <td data-bbox="632 959 947 1052">Enable Always On VPN</td><td data-bbox="947 959 1808 1052">Enable Always On VPN for specified apps in a Work Profile to ensure they always go through a configured VPN.</td></tr> </tbody> </table> </div> <p data-bbox="636 1081 1808 1101">https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features`</p>	Feature	Description	Configure Wi-Fi settings	Remotely deploy Wi-Fi login settings (SSID, password) to a device.	Configure certificate-authenticated Wi-Fi	Remotely deploy Wi-Fi settings to a device that include identity, certificates for client authorization, and CA certificates.	Restrict access to authorized accounts	Ensure that only authorized corporate accounts can interact with Work Profiles data by preventing users from adding or modifying accounts.	Manage certificates	Deploy identity certificates and certificate authorities to a device to enable access to corporate resources.	Manage advanced certificate details	Select certificates for specific work apps, remove CAs and identity certs from an active device, and <u>prevent users from modifying credentials in the managed keystore.</u>	Enable Always On VPN	Enable Always On VPN for specified apps in a Work Profile to ensure they always go through a configured VPN.
Feature	Description														
Configure Wi-Fi settings	Remotely deploy Wi-Fi login settings (SSID, password) to a device.														
Configure certificate-authenticated Wi-Fi	Remotely deploy Wi-Fi settings to a device that include identity, certificates for client authorization, and CA certificates.														
Restrict access to authorized accounts	Ensure that only authorized corporate accounts can interact with Work Profiles data by preventing users from adding or modifying accounts.														
Manage certificates	Deploy identity certificates and certificate authorities to a device to enable access to corporate resources.														
Manage advanced certificate details	Select certificates for specific work apps, remove CAs and identity certs from an active device, and <u>prevent users from modifying credentials in the managed keystore.</u>														
Enable Always On VPN	Enable Always On VPN for specified apps in a Work Profile to ensure they always go through a configured VPN.														

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 13 – U.S. Patent No. 9,294,470

Claims	Identification								
	<p>Responsive to a device being enrolled in Android Enterprise Work Profile and a policy to prevent modification of work profile certificates being enabled, user interface interaction on the device is disabled for importing certificates into the work profile certificate store.</p> <div><p>4.9. Advanced certificate management</p><table><tr><th>Android version</th><th>Work profile</th><th>Fully managed device</th><th>Dedicated device</th></tr><tr><td>7.0+</td><td>★</td><td>★</td><td>★</td></tr></table><p>Allows IT admins to silently select the certificates that specific managed apps should use. This feature also grants IT admins the ability to remove CAs and identity certs from active devices, and prevent users from modifying credentials stored in the managed keystore.</p><p>4.9.1. For any app distributed to devices, IT admins can specify a certificate the app will be silently granted access during runtime. <i>(This subfeature is not currently supported)</i></p><ul style="list-style-type: none">• Certificate selection must be generic enough to allow a single configuration that applies to all users, each of which may have a user-specific identity certificate.<p>4.9.2. IT admins can silently remove certificates from the managed keystore.</p><p>4.9.3. IT admins can silently uninstall a CA certificate. <i>(This subfeature is not currently supported)</i></p><p>4.9.4. IT admins can prevent users from configuring credentials (go to <code>credentialsConfigDisabled</code>) in the managed keystore.</p><p>4.9.5. IT admins can pre-grant certificates for work apps using ChoosePrivateKeyRule.</p></div> <p>https://developers.google.com/android/work/requirements</p>	Android version	Work profile	Fully managed device	Dedicated device	7.0+	★	★	★
Android version	Work profile	Fully managed device	Dedicated device						
7.0+	★	★	★						